

REMARKS

Claims 1, 3, 10, and 15 are amended, no claims are canceled, and no claims are added; as a result, claims 1-15 are now pending in this application.

No new matter has been introduced through the proposed amendments to claims 1, 3, 10, and 15. Support for the proposed amendments to claims 1, 3, 10, and 15 may be found throughout the specification, including but not limited to the specification at page 2, lines 16-19.

Amendments proposed to claims 1, 3, 10, and 15 are admissible because 37 C.F.R. § 1.116(b)(2) states,

(b) After a final rejection or other final action (§ 1.113) in an application or in an ex parte reexamination filed under § 1.510, or an action closing prosecution (§ 1.949) in an inter partes reexamination filed under § 1.913, but before or on the same date of filing an appeal (§ 41.31 or § 41.61 of this title):

(2) An amendment presenting rejected claims in better form for consideration on appeal may be admitted;

Applicant respectfully submits that these proposed amendments to claims 1, 3, 10, and 15 present these claims in a better form for consideration on appeal, and thus may be admitted.

Applicant respectfully requests that these proposed amendments to claims 1, 3, 10, and 15 be entered. In addition, Applicant respectfully requests that the proposed amendments be considered in view of granting an allowance of all claims now pending in the application.

§102 Rejection of the Claims

Claims 1-15 were rejected under 35 U.S.C. § 102(e) for anticipation by Graunke et al. (U.S. 5,991,399). Applicant respectfully traverses the rejection of claims 1-15.

Applicable Law

Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration. *W. L. Gore & Assocs. v. Garlock*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). It is not enough, however, that the prior art reference discloses all the claimed elements in isolation. Rather, A[a]nticipation requires the

presence in a single prior reference disclosure of each and every element of the claimed invention, *arranged as in the claim.*@ *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 221 USPQ 481, 485 (Fed. Cir. 1984) (citing *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 220 USPQ 193 (Fed. Cir. 1983)) (emphasis added). AThe identical invention must be shown in as complete detail as is contained in the ... claim.@ *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); MPEP ' 2131.

"For a prior art reference to anticipate a claim, the reference must disclose each and every element of the claim with sufficient clarity to prove its existence in the prior art . . . Although this disclosure requirement presupposes the knowledge of one skilled in the art of the claimed invention, that presumed knowledge does not grant a license to read into the prior art reference teachings that are not there." *Motorola, Inc. v. Interdigital Tech. Corp.*, 43 USPQ2d 1481, 1490 (Fed. Cir. 1997).

Arguments

Claims 1-15 are not anticipated by Graunke et al. because Graunke et al. fails to disclose in a single prior art reference each of the elements included in any one of claims 1-15, and fails to disclose the identical invention in as complete detail as is included in any one of claims 1-15. Thus, the Final Office Action fails to meet its burden for establishing a *prima facie* case of anticipation with respect to claims 1-15.

By way of illustration, independent claim 1 includes,

System for providing encrypted data to be used in a content player comprising a decryption device, comprising:
an encryption device for encrypting data using an encryption algorithm,
a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and
a control device for providing a protected contents structure containing the encrypted data, the secure device data,

said protocol information and attribute data for finding relevant parts inside the protected contents structure,

wherein the attribute data comprises information to find in the protected contents structure information on **an appropriate protocol for establishing a communication interface using said information on the appropriate protocol between the content player and the secure device for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data.** (Emphasis added).

Thus, independent claim 1 includes, "a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device." Independent claim 1 further includes, "attribute data comprises information to find in the protected contents structure information on an appropriate protocol for establishing a communication interface **using said information on the appropriate protocol** between the content player and the secure device for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data." (Emphasis added).

Independent claim 1 has been amended with this response to emphasize the use of information on the protocol in the communication interface between the content player and a secure device. This subject matter as included in independent claim 1 is not disclosed by Graunke et al., and for at least these reasons independent claim 1 is not anticipated by Graunke et al.

In contrast to independent claim 1, Graunke et al. concerns the distribution of a private key to a user's application program, also called a "trusted player" such as a DVD player, with conditional access on the basis of verification of the trusted player's integrity and authenticity. The private key in Graunke et al. is downloaded from a server to the trusted player in a secure manner. The key is wrapped into a key module in which the key can only be used by the right trusted player as determined by the key module.¹

¹ See Graunke et al. at column 3, line 53 through column 4, line 7.

However, there is no disclosure in Graunke et al. of a secure device as included in the presently claimed subject matter, and so there is no disclosure in Graunke et al. of "a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data," wherein "the attribute data comprises information to find in the protected contents structure information on an appropriate protocol for establishing a communication interface **using said information on the appropriate protocol** between the content player and the secure device for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data," as required by independent claim 1. (Emphasis added).

In an attempt to supply this subject matter, the Final Office Action states that Graunke et al. discloses providing a key module as an interface or applet (plug-in) that provides protocol information to the executable of a trusted player.² Applicant respectfully disagrees that any key module included in Graunke et al. provides or relates to providing protocol information. The portion of Graunke et al. cited in the Final Office Action with respect to this subject matter states,³

This function creates a tamper resistant key module 52 containing the keys necessary to decrypt the selected encrypted content 36 and code to validate the trusted player. The key module also includes an integrity verification kernel (IVK) that, when executed by client 32, will attempt to validate the trusted player. The IVK checks that the trusted player accessing the key module on the client is the correct trusted player according to the manifest and that it has not been altered since purchase and installation by the user.

The key module is forwarded over communications network 34 to client 32. It is a "plug-in" to executable 44 of trusted player 42. The key module is generated to work with a specific trusted player as identified by the user's request and manifest, and also is unique for specific, user-selected digital content.

² See the Final Office Action at pages 2-3 under item 2.

³ See Graunke et al. at column 7, lines 30-45.

Thus, according to Graunke et al. the key module contains:

- the keys necessary to decrypt the selected encrypted content and code to validate the trusted player;
- an integrity verification kernel (IVK) that, when executed by client, will attempt to validate the trusted player by checking that the trusted player accessing the key module on the client is the correct trusted player according to the manifest and that it has not been altered since purchase and installation by the user.

The key module in Graunke et al. is generated to work with a specific trusted player as identified by the user's request and manifest, and also is unique for specific, user-selected digital content. The wording “to work with” as used in Graunke et al. is misinterpreted in the Final Office Action as being related to protocol information.

The correct interpretation is as follows. The key module checks the integrity and authenticity of the trusted player and the IVK in the key module verifies that the signature of the trusted player corresponds to the manifest.⁴ To accomplish this, when the IVK in the key module is being executed by the client, it calculates the digest of the trusted player and compares the calculation to the digest in the manifest. If the IVK in the key module validates the manifest and the trusted player, then the key module is allowed to decrypt the encrypted digital content.⁵ Thus, in Graunke et al. the elements contained in the key module and the wording “to work with” are not related to *protocol information*, but are related to the integrity and authenticity of *the trusted player*.

For at least the reasons stated above, Graunke et al. fails to disclose all of the subject matter included in independent claim 1, and so independent claim 1 is not anticipated by Graunke et al.

In further illustrations of subject matter included in claims 1-15 and not disclosed by Graunke et al.:

Independent claim 3 includes,

System for decrypting encrypted data in a content player,
comprising:

⁴ See Graunke at column 8, lines 39-40

⁵ See Graunke at column 8, lines 40-46.

an input for receiving protected contents containing encrypted data, secure device data, information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and attribute data for finding relevant parts inside the protected contents, a decryption device, and a control device, wherein said secure device data comprises the information required to decrypt the encrypted data, and wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player and the secure device for retrieving the information required to decrypt the encrypted data, **wherein the control device is programmed to use the attribute data to find the appropriate protocol information to establish a communication interface using said information on the appropriate protocol between the decryption device and a secure device** used with the content player, wherein the decryption device is suitable for communicating with the secure device as controlled by the protocol information to obtain the information required by the decryption device to decrypt the encrypted data and generated by the secure device by transforming secure device data communicated to the secure device through the communication interface. (Emphasis added).

Independent claim 10 includes,

Method for providing a communication interface between a decryption device and a secure device in a content player, comprising:

receiving a protected contents structure containing secure device data, information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and attribute data for finding relevant parts inside the protected contents structure, wherein said secure device data comprises the information required to decrypt the encrypted data, the attribute data comprising information to find in the protected contents structure information on an appropriate protocol for communication between the content player and the secure device for retrieving the information required to decrypt the encrypted data, and

retrieving said protocol information from the protected contents structure to establish a communication interface using said information on the appropriate protocol between the decryption device and a secure device used with the contents player to transform secure device data communicated to the secure device through the communication interface into information required by the decryption device to decrypt encrypted data. (Emphasis added).

Independent claim 15 includes,

Method for broadcasting protected contents, comprising:
encrypting data using an encryption algorithm,
providing secure device data,
providing information on a protocol for establishing a communication interface using said information on the appropriate protocol between a content player and a secure device arranged to transform the secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data,
providing protected contents containing the encrypted data, the secure device data, the protocol information and attribute data,
and
broadcasting the protected contents,
wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player and the secure device. (Emphasis added).

For reasons analogous to those stated above with respect to independent claim 1, Graunke et al. fails to disclose all of the claimed subject matter included in independent claim 3, and fails to disclose all of the claimed subject matter included in independent claim 10, and fails to disclose all of the claimed subject matter included in independent claim 15. Therefore, independent claims 3, 10, and 15 are not anticipated by Graunke et al.

Claim 2 depends from independent claim 1, claims 4-9 depend from independent claim 3, and claims 11-14 depend from independent claim 10. Thus, dependent claims 2, 4-9, and 11-14 include all of the claimed subject matter included in the independent claim from which they

depend, and more. For at least the reasons stated above with respect to independent claims 1, 3, and 10, dependent claims 2, 4-9, and 11-14 are not anticipated by Graunke et al.

Because the Final Office Action fails to show how Graunke et al. discloses all of the claimed subject matter included in claims 1-15, the Final Office Action fails to meet its burden for establishing a *prima facie* case of anticipation with respect to claims 1-15. Applicant respectfully requests withdrawal of the 35 U.S.C. § 102 rejection, and allowance of claims 1-15.

Reservation of Rights

In the interest of clarity and brevity, Applicant may not have addressed every assertion made in the Final Office Action. Applicant's silence regarding any such assertion does not constitute any admission or acquiescence. Applicant reserves all rights not exercised in connection with this response, such as the right to challenge or rebut any tacit or explicit characterization of any reference or of any of the present claims, the right to challenge or rebut any asserted factual or legal basis of any of the rejections, the right to swear behind any cited reference such as provided under 37 C.F.R. § 1.131 or otherwise, or the right to assert co-ownership of any cited reference. Applicant does not admit that any of the cited references or any other references of record are relevant to the present claims, or that they constitute prior art. To the extent that any rejection or assertion is based upon the Examiner's personal knowledge, rather than any objective evidence of record as manifested by a cited prior art reference, Applicant timely objects to such reliance on Official Notice, and reserves all rights to request that the Examiner provide a reference or affidavit in support of such assertion, as required by MPEP § 2144.03. Applicant reserves all rights to pursue any cancelled claims in a subsequent patent application claiming the benefit of priority of the present patent application, and to request rejoinder of any withdrawn claim, as required by MPEP § 821.04.

Serial Number: 09/763,732

Dkt: 2069.001US1

Filing Date: February 27, 2001

Title: SYSTEM FOR PROVIDING ENCRYPTED DATA, SYSTEM FOR DECRYPTING ENCRYPTED DATA AND METHOD FOR PROVIDING A COMMUNICATION INTERFACE IN SUCH A DECRYPTING SYSTEM

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney 408-278-4042 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

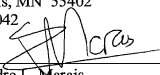
Respectfully submitted,

WILHELMUS GERARDUS PETRUS MOOIJ

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date June 21, 2007

By 
Andre L. Marais
Reg. No. 48,095

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 21st, day of June, 2007.

Dawn R. Shaw
Name


Signature